FSS satellites move across the sky, requiring that an earth station track and utilize multiple satellites to maintain continuity of service. As a result, particular frequencies are effectively unused in directions other than the instantaneous direction in which an earth station is pointed. Using commercially available software tools, information about the satellite system and its orbit parameters, sensed information about the RF environment, or direct information about the satellite system, the direction of the earth stations' transmission or reception could be identified, allowing some users to share frequencies in directions that could be identified for coordinated use.

72. Various cognitive techniques could be used to facilitate coordination and increase spectrum reuse by performing necessary engineering analysis and other frequency coordination tasks in near real-time. We note that our existing framework, and industry practices, for NGSO FSS sharing rely on such dynamic coordination techniques.[80] For example, such tools and technologies could be used to perform engineering analysis to identify desired to undesired signal ratios for terrestrial and satellite links, because satellite orbit parameters, desired time period, and locations of terrestrial links and earth station are known or calculable. The actual occurrence of "worst case" interference conditions could be anticipated and avoided by changing terrestrial paths, changing satellite uplink or downlink paths, modifying RF parameters, or through other techniques. Using cognitive radio technology, one could have FS links in areas that would otherwise not be available under static coordination procedures (such as within certain distances of FSS earth stations). For example, terrestrial operations that occasionally operate near NGSO earth stations could potentially improve their spectral access by agreeing to employ technologies that would anticipate interference and modify or cease operations on a given path and reroute traffic via different paths (using known poly-grid approaches) to prevent that interference.[81] Alternatively, predicted interference could be avoided if the NGSO satellite earth station could change or "hand-off" to a different satellite when the NGSO signal path was approaching that of the terrestrial fixed

(Continued from previous page)
Report and Order and Fourth Notice of Proposed Rulemaking, FCC 96-311 at 11-12, para. 27 (rel. July 22, 1996). The Commission has also allocated NGSO FSS spectrum in the Ku-band where NGSO FSS uplink and downlink operations coordinate with existing terrestrial. *See generally Amendment of Parts 2 and 25 of the Commission's Rules to Permit Operation of NGSO FSS Systems Co-Frequency with GSO and Terrestrial Systems in the Ku-Band Frequency Range,* FCC 00-418, *First Report and Order and Further Notice of Proposed Rule Making,* ET Docket No. 98-206, 16 FCC Rcd 4096 (rel. Dec. 8, 2000) (*NGSO FSS R&O*). NGSO FSS downlink operations share with FS operations in the 10.7-11.7 GHz band, and NGSO FSS downlink operations share with BAS and CARS operations in most parts of the 12.75-13.25 GHz band. *Id.*

[80] To prevent interference when satellites from two NGSO FSS satellite systems align above an earth station, such systems potentially rely on at least three cognitive capabilities. When such an alignment is detected or predicted by an NGSO system, the system can avoid interference by using: different frequencies, alternative satellites in their respective systems, or alternative polarizations. *See* ITU-R S.1431; *In the matter of the Establishment of Policies and Service Rules for the Non-Geostationary Satellite Orbit, Fixed Satellite Service in the Ku Band,* IB Docket No. 01-96, *Report and Order and Further Notice of Proposed Rulemaking*, FCC 02-123, 17 FCC Rcd 7841, 7857, para. 53 (2002).

[81] Polygrid, or mesh, networks emphasize the use of multiple nodes to create a large number of possible paths to connect two or more endpoints. The multiple connectivity of such networks allow endpoints to be connected even when some individual links have to be turned off to prevent interference to or from NGSO satellite systems. *See generally* Harry G. Barker III , David A. Calabrese, David A. Garbin, J. Edward Knepley, Dr. Martin J. Fischer, and Dr. Gregor W. Swinsky, The Circuit Switched Network Design and Analysis Model: A Chronology of Its Development and Use, published in the 2000 The Telecommunications Review (discussing defense applications of polygrid routing features in wireline networks), *available at* http://www.mitretek.org/pubs/telecom/review00/article8.doc.

system. Thus, by adding cognitive radio capabilities in the terrestrial or satellite systems, or both, it can become possible to increase spectrum sharing beyond what it is otherwise possible. Furthermore, cognitive capabilities could improve sharing among terrestrial users as well.

73. We seek comment on ways that we may encourage the use of dynamic coordination approaches. For example, what incentives or regulatory frameworks for dynamic coordination approaches might facilitate satellite and terrestrial coordinated sharing. What coordination procedures would be appropriate for terrestrial to terrestrial sharing? Could satellite providers employ a spectrum reversion mechanism discussed above to permit real-time coordinated use without unreasonable risk of interference to their operations? Would financial incentives encouraging dynamic coordination approaches be warranted? Could our secondary market spectrum leasing provide a framework for such financial incentives? Would explicitly making dynamic coordination an option in our existing coordination procedures be in the public interest?

2. Facilitating Interoperability between Communication Systems

74. An important focus of the Commission has been the facilitation of interoperability among non-federal public safety entities. Cognitive radio technologies offer urgently needed solutions to the increasingly crucial interoperability demands facing first-responders and other licensed users.[82] The Act and our rules currently provide a regulatory framework for interoperability.[83] This framework includes various Commission efforts to facilitate interoperability between non-federal entities at the national, regional, state-wide and local level.[84] Also of importance is interoperability between non-

[82] Wide agreement exists among expert commissions, official reports and other documents on the critical need to provide first responder and emergency management agencies at the Federal, State and local levels with interoperable communications systems to enable them to coordinate response and recovery efforts. *See e.g,* Intergovernmental Dimensions of Domestic Preparedness, Harvard Executive Session Memorandum, Appendix H, Third Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction; A National Action Plan for Safety and Security in America's Cities, The United States Conference of Mayors, December 2001; Institute for Security Technology Studies at Dartmouth College, The First Line of Defense: Tools and Technology Needs of America's First Responders in the Aftermath of September 11, 2001, available at http://www.ists.dartmouth.edu/iria/fld/fld_draft.pdf.

[83] Section 154(o) states "[f]or the purpose of obtaining maximum effectiveness from the use of radio and wire communications in connection with safety of life and property, the commission shall investigate and study all phases of the problem and the best methods of obtaining the cooperation and coordination of these systems." 47 U.S.C. § 154(o); *see also* 47 U.S.C. § 151. Interoperability among public safety systems is defined in Section 90.7 of our rules as "[a]n essential communication link within public safety and public service wireless communications systems which permits units from two or more different entities to interact with one another and to exchange information according to a prescribed method in order to achieve predictable results." 47 C.F.R. § 90.7. Our rules currently provide for interoperability in some bands and define standards for such communications. *See e.g.* 47 C.F.R. § 90.547 (requiring mobile and portable transmitters operating in 764-776 & 794-806 MHz be capable of operating on all designated nationwide narrowband interoperability channels); 47 C.F.R. § 90.548 (defining technical standards for narrowband interoperability channels); 47 C.F.R. § 90.549 (requiring transmitters operating in 764-776 & 794-806 MHz bands be certified as required by general technical requirements for Part 90).

[84] The frequencies include 2.6 MHz of the 700 MHz band, 5 channels in the 800 MHz band, 5 channels in the 150 MHz band (VHF band), and 4 channels in the 450 MHz band (UHF band). Among these frequencies, five channels are designated for nationwide interoperability communications. Regional planning committees address a variety of interoperability frequency planning at the regional level. Under this framework States administer (continued....)

federal public safety entities and federal government first responders. For instance, the Commission has provided for federal government entities' use of 700 MHz public safety spectrum when used for interoperable communications.[85] In addition, non-federal public safety entities sometimes use frequencies allocated to federal government use.[86] The Commission has continued to broaden this framework in the context of other proceedings by designating new spectrum for public safety interoperable use, for instance in the DTV transition where 2.6 MHz of the 24 MHz of added spectrum is reserved for public safety interoperable use.[87] Despite these efforts, lack of interoperability has been identified as a significant problem in the response to several disasters involving multiple jurisdictions, such as the September 11, 2001, attack on the Pentagon and the 1982 Air Florida crash.[88] Cognitive radio technologies addressed in this proceeding offer a new means of reducing risks to safety of life and national security by increasing the opportunities for first responders interoperability.

75. Both industry and government bodies are actively addressing the complex issues posed by the need for interoperable communication between public safety entities. The Public Safety National Coordination Committee (NCC) recently made recommendations on interoperability and other related issues in their report to the Commission.[89] The Commission's Office of Homeland Security is also exploring potential changes to the Commission's technical rules, policies, procedures, or practices that would facilitate development of cognitive radio technology to enhance public safety communications.[90]

76. Cognitive radio devices' capability to automatically or with some user input identify systems and users that need bridging, could facilitate interoperability under our existing regulatory framework. Devices capable of sensing and identifying signals could dynamically respond to new

(Continued from previous page)

interoperable spectrum on the state level. 47 CFR § 90.525(a) ("States are responsible for administration of the Interoperability channels in the 764-776 MHz and 794-806 MHz frequency bands.").

[85] *See e.g.* 47 C.F.R. § 2.103(b).

[86] For instance, non-federal responders from Montgomery County, Maryland Fire & Rescue; Prince William county, Virginia, Fire & Rescue; Virginia State Police; Virginia Department of Transportation; and numerous federal responders including the F.B.I. and U.S. Park Police Public operate across the entire span of the 138-174 MHz band. *See* Public Safety Wireless Network Program, Answering the Call: Communications Lessons Learned from the Pentagon Attack at 7-8 Table 1 and Map 1 (January 2002), available at http://www.pswn.gov/admin/librarydocs7/Answering_the_Call_Pentagon_Attack.pdf (summarizing communication systems used by jurisdictions responding to Pentagon attack).

[87] *See generally The Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communication Requirements through the Year 2010*, WT Docket No. 96-86, *First Report and Order and Third Notice of Proposed Rulemaking*, 14 FCC Rcd 152 (1998).

[88] Interoperability was a serious concern in the response to the terrorist attack on the Pentagon. *See* Federal Emergency Management Agency, Managing the Emergency Consequences of Terrorist Incidents, INTERIM PLANNING GUIDE FOR STATE AND LOCAL GOVERNMENTS 25 n.9. (July 2002), available at http://www.fema.gov/pdf/onp/managingemerconseq.pdf. Interoperability was also a serious problem for first responders to the crash of Air Florida flight 90 in 1982 that resulted in 78 deaths under the 14th street bridge just miles from the Pentagon.

[89] *See* Letter from Kathleen M.H. Wallman to Michael Powell, Chairman, Federal Communications Commission, WT Docket No. 96-86 (July 25, 2003) [hereinafter NCC *ex parte*].

[90] FCC Homeland Security Action Plan (July 10, 2003), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-236428A2.doc.

jurisdictions seeking to deploy interoperable systems. Devices could, in real time, adapt waveforms received from one system and change their modulation formats (such as APCO25 to FM) and frequencies and facilitate interoperability with other systems. For example, during their response to the Pentagon attack, Arlington County Fire's ability to communicate with firemen reporting from other jurisdiction would not have been limited to their supply of radios to distribute. A device could simply have bridged communications from any jurisdictions arriving with their own radios. Cognitive radio devices could also be used to connect to password protected databases available for public safety use that could help identify the kinds of frequencies and waveforms that dynamic interoperability would need to bridge.[91] Devices could also perform this interoperability bridging using encryption technology when secure communications are required.[92] Such a feature might be very useful for federal entities utilizing secure communications systems that assume responsibility for coordinating rescue and response efforts. FBI entities who assume control of coordinating such efforts may need to bridge from secure communication systems in order to communicate with certain non-federal entities. Cognitive radios may also contribute to the provision of E911 by providing a bridge between systems using different air interfaces to provide wireless E911 services. We seek comment on how cognitive radio technologies can facilitate interoperability between systems. We also seek comment on any rule changes necessary to take advantage of these benefits for interoperability between systems.[93] We also seek comment on how cognitive radio technologies can provide support to wireless E911 services.

3. Mesh Networks

77. Emerging technologies, such as "mesh" networks, rely on each node in an RF network to collect and disseminate information and optimize spectrum use by relaying messages through the RF network.[94] We seek comment on the application of this technology and possible rule changes needed to facilitate the use of these technologies.

78. In a mesh network, each transmitter interacts on a peer-to-peer basis with other nearby transmitters, while also sending and receiving messages mimicking a router that relays messages to and from neighboring transmitters. Through this relaying process, a message can be routed through other transmitters to its destination based on the current conditions of the network. The received power at an antenna is reduced as the distance from a transmitter increases, and thus more power is required to transmit to a receiver farther away. Mesh networks function by "whispering" at low power to a neighbor rather than "yelling" at a high-power to a node far away. This approach may be spectrally more efficient

[91] To date, the Commission has declined to require the use of a password protected pre-coordination data base in the regional planning process. *See* The Development Of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010, WT Docket No. 96-86, *Fourth Memorandum Opinion and Order*, 17 FCC Rcd. 4736, 4737 (2002). However, the NCC urges the Commission to review this decision and mandate its use. *See NCC ex parte* at 6.

[92] Our rules currently permit encrypted communication on all but two national channels reserved for interoperability. *See* 47 C.F.R. § 90.533(a).

[93] The NCC recommended that the Commission amend Section 90 of its Rules to include a new section titled "Interoperability Channels: Administration, Use, Limitations" that would consolidate existing rules governing interoperability and any new rules that the Commission may adopt in response to the NCC's recommendations. *See NCC ex parte* at 6.

[94] *See* FCC Tutorial, Wireless Ad Hoc Mesh Network Technology, DA 02-1201, *Public Notice* (rel. May 20, 2002).

than simply transmitting directly to a desired receiver at some distance and provide for better sharing scenarios. We seek comment how such techniques could be applied to facilitate our goals of improved spectrum sharing.

79. Mesh networks can allow radio use to expand to areas beyond the reach of network base stations, yet enable multiple users to avoid interference to each other. This capability could make it possible to deploy operations in areas where line of site is obstructed or unavailable and the propagation characteristics of the band would otherwise require unobstructed line of site. For example, such a capability could be helpful for both licensed and unlicensed operations in the microwave bands where common obstructions such as trees limit the ability to deploy services with low power. We seek comment how this technology might serve our efforts to facilitate broadband communication services to consumers, and any rule changes that might be necessary. We also seek comment on the impact that mesh networks will have on the aggregate interference to licensed services.

80. The ability of mesh networks to "self-heal" by responding to failures in the network may offer important benefits for ensuring network reliability. If one link in a mesh network fails, a message can be routed to its destination through alternate links. In this way all transmissions from the nodes of a mesh network operate in coordinated manner, in the same manner that Internet routers intelligently respond to outages by routing traffic around failures. We seek comment on how such capabilities could improve the reliability of wireless operations.

E. SDR and Cognitive Radio Equipment Authorization Rule Changes

1. Background

81. Most radio transmitters are required to be certified before they can be marketed within the United States and Part 2 of the FCC rules specifies the procedures for obtaining certification for both licensed and unlicensed transmitters.[95] The certification rules require that the equipment be tested to show compliance with the applicable technical rules, and that an application, test report and certain exhibits be filed with either the Commission or a designated Telecommunication Certification Body (TCB).[96] The rules also provide that when any changes are made to the operating frequency range, modulation type or maximum output power of an approved device the manufacturer must file a new application for certification.[97] The rules permit certain changes to an approved device to be made though a "permissive change" procedure. The permissive change rules require manufacturers to submit either a streamlined filing or no filing and do not require manufacturers to place a new identification number on a device.[98]

[95] *See* 47 C.F.R. Part 2, subpart J.

[96] *See* 47 C.F.R. §§ 2.1033 and 2.960.

[97] *See* 47 C.F.R. § 2.1043(a).

[98] *See* 47 C.F.R. § 2.1043(b). There are three classes of permissive changes. A Class I permissive change includes minor modifications to a device that do not degrade the characteristics measured at the time of certification. No filing is required for a Class I change. A Class II permissive change includes modifications to a device that degrade the characteristics measured at the time of certification, although the device must continue to comply with the applicable rules. Manufacturers must supply information on the Class II changes to the Commission or TCB and must receive an acknowledgement from the Commission or TCB that the changes are acceptable before the modified equipment may be marketed. A Class III permissive change includes modifications to the software in a (continued....)

82. In 2001, the Commission adopted changes to the equipment authorization rules to accommodate the developing software defined radio (SDR) technology.[99] The Commission defined a software defined radio as a transmitter in which the operating parameters of frequency range, modulation type, or maximum output power (either radiated or conducted) can be altered by making a change in software that controls the operation of the device without making any changes in the hardware components that affect the radio frequency emissions.[100] Although this broad definition covers both radios that have software imbedded on chips when the software can not be readily changed by the user as well as radios that are designed so the software can be easily changed after manufacture, the primary focus of this item is on the latter category. Possible ways to load new software into a radio after manufacture include over the air, through a connection to a personal computer or other programming device, and by replacement of a card or chip.

83. The SDR rules were intended to make possible for manufacturers to obtain approval for changes to the operating parameters of a radio resulting from software changes without the need to physically re-label a device with a new FCC identification number in the field. The Commission made the rules permissive, rather than mandatory, thereby permitting a manufacturer the option to his declare a device an SDR at the time of filing for certification, but not requiring the manufacturer to do so. The Commission adopted the following rule changes for SDRs:

- Established a new streamlined procedure for obtaining approval for changes to the operating parameters of SDRs that result from changing the software in the device.[101] The same FCC identification number may be used when changes are made to an approved device.
- Allowed a device's FCC identification number to be displayed electronically, rather than on a physical label.[102]
- Required SDRs to incorporate security features to ensure that only software that is part of an approved hardware/software combination can be loaded into an SDR. The exact methods are left to the manufacturer.[103]
- Required manufacturers to supply a copy of the software that controls the operating parameters of a radio to the Commission upon request.[104]

84. Although the SDR rules were adopted over two years ago, to date no manufacturers have filed applications to certify a device under our new SDR rules. However, devices have been certified that

(Continued from previous page)
software defined radio that change the frequency, modulation type, output power or maximum field strength outside the parameters previously approved. Manufacturers must submit a description of the Class III changes and test results showing that the equipment complies with the applicable rules with the new software loaded to the Commission and must receive an acknowledgement that the changes are acceptable before the modified equipment may be marketed. TCBs are currently not permitted to certify SDRs.

[99] *See First Report and Order* in ET Docket No. 00-47, 16 FCC Rcd 17373 (2001).

[100] *See* 47 C.F.R. § 2.1.

[101] *See* 47 C.F.R. § 2.1043(b)(3).

[102] *See* 47 C.F.R. § 2.925(e).

[103] *See* 47 C.F.R. § 2.932(e).

[104] *See* 47 C.F.R. § 2.944.

would meet the Commission's broad definition of an SDR, but the manufacturer did not choose to declare them as such at the time of certification. We, therefore, do not know whether these devices incorporate features to prevent unauthorized changes to the operating parameters because there is no requirement to incorporate security features in a transmitter that is not declared as an SDR. Thus, we are concerned about the potential for parties to make unauthorized changes to software programmable radios after they are manufactured and first sold which could result in harmful interference to authorized services. Further, we note that manufacturers are now developing transmitters that are "partitioned" into two or more physical sections connected by wires, where one section houses the control software and another contains the RF transmission functions.[105] We, therefore, believe it is time to revisit the SDR rules to determine if changes are needed concerning whether the SDR rules should be permissive or mandatory, the types of security features that an SDR must incorporate, and the approval process for SDRs that are contained in modular transmitters.

2. Proposals for Part 2 rule changes

85. *Submission of radio software.* The rules requires the applicant, grantee, or other party responsible for compliance of an SDR to submit a copy of the software source code that controls the device's radio frequency operating parameters to the Commission upon request.[106] This requirement is analogous to the requirement to supply photographs and circuit diagrams for hardware based devices and was added to assist in enforcement by allowing the Commission's staff to obtain information it could examine to determine if unauthorized changes had been made.

86. Because of the expected complexity and variations in the programming languages of the software used to control radio operating parameters, examining radio software is unlikely to be an effective way to determine whether unauthorized changes have been made to a device. Source code generally can not be directly compared to the software loaded within a device because the source code is compiled before loading and additional changes to the code may be made in the loading process. Even if there were a way to compare software, manufacturers are permitted to make changes to the software that have no effect on the operating parameters at any time without notice to the Commission, and it could prove difficult for the Commission's staff to determine whether such changes affect the compliance of a device. A high level description of the radio software and flow diagram of how it works would be more useful in understanding the operation of a device than a copy of the software. We therefore propose to delete the requirement that grantees or applicants supply a copy of their radio software upon request, and propose to add a less burdensome requirement that applicants supply a description and flow diagram of the software that controls the radio operating parameters. The existing requirement in the rules that certified equipment must comply with the applicable technical rules appears to be a sufficient safeguard against unauthorized changes to equipment.[107] Further, the rules require that an applicant or grantee supply a sample of a device to the Commission upon request that we can test to determine if a device is

[105] For example, a notebook computer may run software that digitally generates a radio frequency waveform and sends the data to a wireless LAN card that further processes and transmits the radio signal.

[106] *See* 47 C.F.R. § 2.944. Failure to comply within 14 days may be grounds for denial of equipment authorization or monetary forfeitures.

[107] *See* 47 C.F.R. § 2.931.

compliant.[108] Grantees are also required to maintain records of equipment specifications and any changes that may affect compliance, which must be made available for inspection by the Commission.[109]

87. *Applicability of SDR Rules.* As noted above, the current rules allow a manufacturer to declare that a particular radio is an SDR when the application for equipment authorization is filed, but currently do not require this declaration. By not declaring a radio as an SDR, the manufacturer is not required to incorporate the necessary security features to ensure that only software that is part of an approved hardware/software combination can be loaded. This means that a radio can be potentially modifiable, and perhaps easily so, to operate with parameters not permitted by the rules, or to operate outside those that were approved for the device, thus increasing the risk of interference to authorized radio services. However, not all radios that meet the broad definition of an SDR are easily modifiable after manufacture. For example, many radios incorporate software on chips that can not be reprogrammed or easily replaced by a user.

88. We seek comment on the need for a requirement that manufacturers/importers declare certain equipment as SDRs, including the benefits of such a requirement in reducing interference and its possible burdens on manufacturers. We also seek comment on the types of devices to which this requirement should apply, including how the rules should distinguish between transmitters that must be identified as SDRs and those that need not be. Our goal for such a requirement is to minimize the possibility of unauthorized operation of software programmable radios, yet avoid imposing new requirements on manufacturers whose equipment meet the definition of SDR but are designed in a manner such that the transmission control software is not easily modified. For example, should we require that transmitters into which software can be loaded to change the operating parameters after manufacture be declared as SDRs, and that they comply with the requirements for SDRs, including incorporation of a means to prevent unauthorized software changes? Should this requirement apply to transmitters in which the software can be modified through means such as a physical interface to a personal computer or other device, an over-the-air download, use of a keypad or buttons on the device, or by replacing a board, card or chip that is not permanently attached to the device? Should this requirement apply to radios that can only be reprogrammed by the manufacturer or service center using proprietary software that has some form of security protection?

89. We further seek comment on whether a requirement to declare certain devices as SDRs should apply to transmitter modules. The Commission recently proposed in a separate proceeding providing manufacturers additional flexibility for authorization of transmitter modules that are partitioned into separate radio front ends and firmware provided they use digital keys to ensure that only a radio front end and firmware that have been certified together may operate together.[110] Would the proposed partitioning and digital key requirements for transmitter modules be sufficient to protect against unauthorized software modifications of modules and eliminate the need to require modules to be declared as SDRs?

---

[108] *See* 47 C.F.R. §§ 2.943 and 2.946.

[109] *See* 47 C.F.R. §§ 2.936(a) and 2.938(a). We note that Sections 303(e) and Section 4(i) of the Communications Act continue to give the Commission authority to request data that will assist us in carrying out our responsibilities under the Act. *See* 47 U.S.C. §§ 154(i) and 303(e).

[110] *See generally In the matter of Modification of Parts 2 and 15 of the Commission's Rules for unlicensed devices and equipment approval*, ET Docket No. 03-201, *Notice of Proposed Rulemaking*, FCC 03-223 (rel. Sep. 17, 2003).

90. Equipment used by amateur radio operators is generally exempt from a certification requirement.[111] We have maintained this policy to encourage innovation and experimentation in the Amateur Radio Service.[112] However, we are concerned that it may be possible for parties to modify SDRs marketed as amateur equipment to operate in frequencies bands not allocated to the Amateur Radio Service if appropriate security measures are not employed. However, we do not wish to prevent licensed amateurs from building or modifying equipment, including SDRs that operate only in amateur bands in accordance with the rules. Accordingly, we propose that manufactured SDRs that are designed to operate solely in amateur bands are exempt from the mandatory declaration and certification requirements, provided the equipment incorporates features in hardware to prevent operation outside of amateur bands. We seek comment on this proposal.

91. At present there is a clear distinction between radio transmitter technology, regulated under Section 2.801(a) of our rules and various radio service rules, and personal computer technology, regulated in a much less restrictive way under Subpart B of Part 15 of our rules. However, increasing computer speeds and speeds of digital-to-analog converters (DAC)[113] may well blur this distinction. A general purpose computer capable of outputting digital samples at rates in the million sample/seconds range or higher could be connected to a general purpose high-power, high-speed DAC card which could effectively function as a radio transmitter. The marketing of such computers, DACs, and software to make them interact could undermine our present equipment authorization program at the risk of increasing interference to legitimate spectrum users since none of them would be subject to the normal authorization requirements. At present this is not a problem, but we wish to consider modest steps now to help ensure that this scenario does not become a serious problem.

92. While such high-speed DACs are presently marketed to the scientific community at high unit costs, we are not aware of any which are marketed as consumer items. We seek comment on whether we need to restrict the mass marketing of high-speed DACs that could be diverted for use as radio transmitters and whether we can do so without adversely affecting other uses of such computer peripherals or the marketing of computer peripherals that cannot be misused. We seek comment on one possible approach as well as welcoming alternative proposals. Would it make sense to require that digital-to-analog converters marketed as computer peripherals that 1) operate at more than one million digital input samples/second, 2) have output power levels greater than 100 mW and, 3) have an output connector for the analog output be limited in marketing to commercial, industrial and business users as we require for Class A digital devices? Would it be preferable to characterize such systems in terms of output frequency and bandwidth rather than input sampling rate? What sampling rate and power limits would be needed to avoid impacting DACs that might have a legitimate consumer use such as, for video systems and other media applications? Is there a practical way to incorporate security features that would limit the frequency range or other operating parameters of these devices? We also seek comment on the specific types of devices that would be affected and the potential burden on manufacturers.

---

[111] Amateur radio equipment is exempt from a certification requirement, except for external power amplifiers operating below 144 MHz. Such amplifiers must have no gain in the 26-28 MHz band to ensure that they can not be used to amplify the output of transmitters operating in the Citizen's Band (CB) Radio Service. *See* 47 C.F.R. §§ 97.315 and 97.317.

[112] *See* 47 C.F.R. § 97.1.

[113] The common personal computer sound card uses a low speed DAC, typically about 40,000 samples/second, to produce audio output.

93. *Security and authentication requirements.* The rules require that manufacturers take steps to ensure that only software that is part of an approved hardware/software combination can be loaded into an SDR.[114] The software must not allow the user to operate the transmitter with frequencies, output power, modulation types or other parameters outside the range of those that were approved.[115] Manufacturers may use authentication codes or any other means to meet these requirements, and must describe the methods in their application for equipment authorization.[116] In adopting these requirements, the Commission stated that it may have to specify more detailed security requirements at a later date as SDR technology develops.[117]

94. We seek comment on whether any modifications are necessary to the security and authentication requirements in the rules. Specifically, we seek comment on whether the current rules provide adequate safeguards against unauthorized modifications to SDRs. We also seek comment on whether more explicit security requirements are necessary, such as requiring electronic signatures in software to verify the software's authenticity. We further seek comment on what should happen in the event that reasonable security methods ultimately are broken. Should there be limits to a manufacturer's responsibility if, for example, the manufacturer follows an accepted industry standard for security?[118] If manufacturers' responsibility is limited, how would the Commission enforce its rules, *e.g.*, if interference occurs, against the users of unauthorized software or the creators/distributors of unauthorized software? At least one party has proposed rule changes to clarify how a manufacturer can comply with the requirements of Section 2.932(e) of our rules, and to define the standard of care to be applied.[119] We seek comment whether defining compliance using "commercially reasonable measures," or some other standard, such as "industry accepted practice," would appropriately balance our goals for ensuring compliance with our rules and burdens on manufacturers. As described above, device with cognitive capabilities may be subject to new forms of abuse to which other devices are not susceptible. Of course, devices with cognitive capabilities would generally require certification by the Commission, and thus are subject to the marketing and use restrictions of Section 2.803.[120] We seek comment on how we can enable the use of cognitive radio technologies, but prevent abuses such as those described above. Are there features that could be incorporated into devices to help detect attempts to physically tamper with spectrum sensing and geo-location technologies built into devices? Could devices be designed to detect alterations to control software or databases and cease operation if such alterations are detected?

---

[114] *See* 47 C.F.R. § 2.932(e).

[115] *Id.*

[116] *Id.*

[117] *See Report and Order* in ET Docket No. 00-47, 16 FCC Rcd 17373, 13383 (2001).

[118] *See* Vanu Inc. Comment, August 1, 2003.

[119] Vanu proposes the following language to clarify compliance with 47 C.F.R. § 2.932(e):

> A manufacturer will be deemed to comply with the first sentence of Section 2.932(e) if it has taken measures that are commercially reasonable in light of standards employed in the software defined radio industry and other analogous industries at the time, provided that it has not marketed a device containing a software vulnerability that was publicly known, or known to the manufacturer, at the time of marketing.

Vanu Inc. Comment, at 2 November 19, 2003.

[120] *See* 47 C.F.R. § 2.803.

3. Proposals for Part 15 rule changes

95. *Automatic frequency selection for unlicensed devices.* Many frequency bands where unlicensed operation is permitted are not harmonized worldwide. For example, in the United States, unlicensed operation is permitted in the 2400-2483.5 MHz band, while in other countries operation is permitted in the 2400-2500 MHz band.[121] The 2483.5-2500 MHz band is used for the Mobile Satellite Service (MSS) in the United States and is a restricted band under Part 15, therefore unlicensed devices are not permitted to transmit in that band to prevent interference to the MSS.[122] Unlicensed transmitters are now being manufactured in which the frequency range of operation can be software selectable. However, a transmitter can not be approved in the United States unless it is capable of complying with the technical requirements of the rule part under which it will be operated.[123] Therefore, an unlicensed transmitter that is capable of operation outside permitted bands of operation under Part 15 of the rules cannot be certified for operation in the United States.

96. Manufacturers would like the ability to certify devices to operate over a wider frequency range than is permitted in the United States, provided the devices incorporate some sort of technology that selects the appropriate operating frequency ranges based on the country in which they are used. A device could limit its operation to authorized frequencies when used in the United States, but could operate on additional frequencies as permitted in other countries. This approach could allow the production of devices that could be used worldwide, or at least in a number of different countries, and eliminate the need for manufacturers to produce multiple versions of a device for use in different countries.

97. Allowing certification of frequency selectable wireless devices could benefit consumers and manufacturers by reducing production costs and allowing production of devices that can be used in both the United States and other countries. We therefore propose to allow certification of Part 15 devices that are capable of operating on non-Part 15 frequencies. We propose to require that such devices incorporate DFS to select the appropriate operating frequency based on the country of operation and must operate on only Part 15 frequencies when used in the United States. In addition, we propose that such devices must incorporate a means to determine the country of operation. There are several methods that a device could use to make this determination. One is to incorporate geo-location capability, such as GPS, combined with a database, to determine the device's geographic location. Alternatively, a device could rely on information provided by another device to determine the country of operation or the permissible frequency band. For example, a device such as a wireless LAN card could rely on a network access point to select the appropriate operating frequency band. Under that scenario, it would be necessary to assure that the network access point is capable of determining its location and communicating that information to a connected device.

98. We seek comment on this proposal; in particular, the means that a device should employ to determine its country of operation and select the appropriate operating frequency range. Are there methods other than the ones described above that could be employed? How should a device respond if it is unable to determine its geographic location? If the frequency band or country of operation is determined by an external device such as a network access point, what specific requirements should

[121] *See* 47 C.F.R. §§ 15.247 and 15.249.

[122] *See* 47 C.F.R. §§ 15.205 and 25.202.

[123] *See* 47 C.F.R. § 2.915(a)(1).

apply to different types of devices used in a system such as wireless LAN cards and network access points? We also seek comment on how to assure that users cannot select an unauthorized frequency range or easily modify devices to operate in unauthorized frequency ranges. Consistent with our proposals above, we seek comment on whether devices in which the operating frequency range can be selected through software should be required to be declared as SDRs, and therefore required to meet the security and authentication requirements for SDRs to prevent unauthorized modifications.

4. Pre-certification testing requirements for cognitive radios

99. Transmitters must be tested to show compliance with the applicable technical requirements before they can be certified. For unlicensed transmitters, both the technical requirements and the test procedures are specified in Part 15 of the rules.[124] For transmitters used in licensed services, the technical requirements are contained in the rule part for a particular service, and the test procedures are specified in Part 2 of the rules.[125] The types of tests specified in these procedures include field strength, output power, spurious emissions, occupied bandwidth and frequency stability.

100. With most transmitters, the output is tested in response to a single or limited number of input conditions to show compliance with the rules for the service(s) in which they will operate. Cognitive radios must also be tested to show compliance with the rules for the services in which they will operate, but unlike other transmitters it may also be necessary to test the output in response to various inputs or various combinations of inputs. Because cognitive radios can perform functions not envisioned at the time the current rules were developed, it may be necessary to specify additional tests to ensure the compliance of cognitive radios. The types of tests to be required will vary depending upon the types of technical requirements specified for a radio in a particular service, and applicants for equipment authorization will be required to provide the results of such testing before certification is granted. We expect that in the near future, any new testing procedures for cognitive radios will be specified at the same time as new cognitive radio rules are adopted as we did in the proceeding making new spectrum available for unlicensed devices in the 5 GHz band. However, it may eventually be necessary to establish a more general framework for testing cognitive radios. As discussed below, we seek comment on the new types of tests that will be required in two broad areas - unlicensed and licensed transmitters.

101. *Tests required for unlicensed devices.* As indicated above, we are proposing to allow unlicensed transmitters to operate at higher power levels in areas with limited spectrum use. In order to make the determination as to when higher power operation is permissible, the transmitter must have the ability to scan the spectrum to determine occupancy. To verify whether a device has the capabilities that we ultimately decide are necessary, there are potentially a number of specific tests that may have to be performed on a specific device. These tests would include:

- Determine the frequency range that can be scanned by device
- Measure the scanning resolution bandwidth
- Determine the sensitivity of the scanning receiver used to examine spectrum occupancy
- Test the ability of the device to correctly determine spectrum occupancy based on presence of various standardized input test signals.

[124] *See* 47 C.F.R. §§ 15.31 through 15.35. These sections specify general testing procedures applicable to unlicensed transmitters. In addition, some industry procedures such as the ANSI C63.4 procedure for measuring emissions from intentional and unintentional radiators are incorporated by reference into the rules.

[125] *See* 47 C.F.R. §§ 2.1046 through 2.1060.

- Determine time period to monitor before declaring that the spectrum is not occupied.
- Ensure transmitter power control adjusts to the correct level.
- Time to revisit a portion of the spectrum to ensure that it is still unused.
- Response time to vacate a portion of the spectrum when it is determined that the spectrum is being used.

102. We seek comment on the above tests as well as on any other tests that may be needed to assure compliance by unlicensed devices with the SDR and any new cognitive radio rules, as well as a more detailed description of the measurement procedures that could be used. For testing a device's response to various standardized input signals, we seek comment on the frequencies, types and levels of the signals that should be used. Should there be a series of input signal tests required, and if so, what should they be? We also seek comment on whether the Commission should develop such test procedures or whether they should be developed through an industry standards organization such as ANSI.

103. *Tests required for interruptible radios.* We discussed above that cognitive radios could conceivably share spectrum with other services, such as public safety or commercial users. Such sharing could be facilitated by use of a reversion mechanism, as proposed for public safety frequencies, that causes the cognitive radio to cease transmission when the primary user of the spectrum needs to use it. The reversion mechanism could be the loss of a beacon signal or there could be some other control signal telling the cognitive radio to cease transmission. In order to assure that the reversion mechanism works properly, certain new tests may be needed for radios using one of these technologies. We seek comment on the testing criteria may be appropriate for an RF beacon based system. Likewise, we seek comment on what testing criteria may be appropriate for beacon systems whose signal is not delivered over the air. We seek comment on whether these tests are appropriate, and whether additional tests should be required:

- Ability of the radio to sense a beacon or other control signal on the appropriate frequency or from another source.
- Minimum receive sensitivity for the control signal.
- Response time to vacate channel when beacon signal is lost or other control signal orders cessation of transmission.

104. *Other required tests specific to cognitive radios.* In addition to the specific cases described above, there may be a need to establish a more general framework for testing cognitive radios. We seek comment on the need for the following tests for different types of cognitive radio technology.

105. Listen-before-talk systems scan one or more frequency ranges to determine whether there are any other users present before transmission. The following tests may be appropriate for listen-before-talk systems:

- Determining the frequency band that is scanned by device
- Measuring the scanning resolution bandwidth
- Sensitivity of the scanning receiver used to determine spectrum occupancy
- Ability of the device to select an operating frequency and power level based the presence of various standardized test input signals.
- Determine time period to monitor before declaring that the spectrum is not occupied.
- Time to revisit a portion of the spectrum to ensure that it is still unused.
- Response time to vacate a portion of the spectrum when it is determined that the spectrum is being used.

We seek comment on the need for these tests and on any other tests that may be needed for listen-before-talk systems. For testing a device's response to various standardized input signals, we seek comment on the frequencies, types and levels of the signals that should be used. Should we require a series of input signal tests, and if so, how many?

106. Geo-location systems use GPS or some other method to determine the transmitter's location. A database can be used to determine the transmitter's proximity to other devices that need to be protected from interference. The following tests may be necessary for devices that use geo-location. We seek comment on the need for these tests and for any other tests that may be required for radios that incorporate geo-location technology:

- Ability to correctly identify its location based on GPS or some other method
- Ability to access database to correctly determine location and authorized operating parameters of other transmitters in the vicinity
- Device response when geo-location signal is lost or can not be found

107. Cognitive radios may allow transmissions using new or novel formats. For example, it may be possible to divide a signal so transmissions occur simultaneously using multiple non-contiguous frequency blocks.[126] Such waveforms could potentially result in more efficient use of spectrum by allowing small unused blocks of spectrum to be "combined" into larger, more useful blocks of spectrum. However, this type of technology raises some novel measurement issues because the Commission did not envision its use when developed the rules. We therefore seek comment on the following questions related to this technology.

- How should the transmit power be measured to determine compliance with the power limits? Should the measurement be of the power per channel, the total power over all channels, or some other measurement?
- How can the bandwidth be measured?
- How should the modulation type be defined?

IV. PROCEDURAL MATTERS

Initial Regulatory Flexibility Analysis

108. As required by the Regulatory Flexibility Act, 5 U.S.C. § 603, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities of the policies and rules proposed in this document. The IRFA is set forth in Appendix C. Written public comments are requested on the IRFA. These comments must be filed in accordance with the same filing deadlines as comments filed in response to this Notice of Proposed Rule Making as set forth in paragraph 111, and have a separate and distinct heading designating them as responses to the IRFA.

Initial Paperwork Reduction Act of 1995 Analysis

109. This Notice contains either a proposed or modified information collection. As part of its continuing effort to reduce paperwork burdens, we invite the general public and the Office of Management and Budget (OMB) to take this opportunity to comment on the information collections

[126] This technology has been referred to as "heteromorphic waveforms".

contained in this Notice, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. Public and agency comments are due at the same time as other comments on this Notice; OMB comments are due 60 days from date of publication of this Notice in the Federal Register. Comments should address: (a) whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information shall have practical utility; (b) the accuracy of the Commission's burden estimates; (c) ways to enhance the quality, utility, and clarity of the information collected; and (d) ways to minimize the burden of the collection of information on the respondents, including the use of automated collection techniques or other forms of information technology.

110. *Ex Parte Presentations*. This is a permit-but-disclose notice and comment rule making proceeding. *Ex parte* presentations are permitted, except during the Sunshine Agenda period, provided they are disclosed as provided in the Commission's rules. *See generally* 47 C.F.R. §§ 1.1202, 1.1203, and 1.2306(a).

111. *Filing Comments*. Pursuant to Sections 1.415 and 1.419 of the Commission's rules, 47 C.F.R. §§ 1.415, 1.419, interested parties may file comments on or before [75 days from publication in Federal Register], and reply comments on or before [105 days from publication in Federal Register]. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS) or by filing paper copies. See Electronic Filing of Documents in Rulemaking Proceedings, 63 Fed. Reg. 24121 (1998).

112. Comments filed through the ECFS can be sent as an electronic file via the Internet to http://www.fcc.gov/cgb/ecfs/. Generally, only one copy of an electronic submission must be filed. If multiple docket or rulemaking numbers appear in the caption of this proceeding, however, commenters must transmit one electronic copy of the comments to each docket or rulemaking number referenced in the caption. In completing the transmittal screen, commenters should include their full name, U.S. Postal Service mailing address, and the applicable docket.or rulemaking number. Parties may also submit an electronic comment by Internet e-mail. To get filing instructions for e-mail comments, commenters should send an e-mail to ecfs@fcc.gov, and should include the following words in the body of the message, "get form ." A sample form and directions will be sent in reply. Parties who choose to file by paper must file an original and four copies of each filing. If more than one docket or rulemaking number appear in the caption of this proceeding, commenters must submit two additional copies for each additional docket or rulemaking number.

113. Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail (although we continue to experience delays in receiving U.S. Postal Service mail).

114. The Commission's contractor, Natek, Inc., will receive hand-delivered or messenger-delivered paper filings for the Commission's Secretary at 236 Massachusetts Avenue, N.E., Suite 110, Washington, D.C. 20002.

-The filing hours at this location are 8:00 a.m. to 7:00 p.m.

-All hand deliveries must be held together with rubber bands or fasteners.

-Any envelopes must be disposed of before entering the building.

-Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.

-U.S. Postal Service first-class mail, Express Mail, and Priority Mail should be addressed to 445 12th Street, SW, Washington, D.C. 20554.

-All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

115. Parties who choose to file by paper should also submit their comments on diskette. Such a submission should be on a 3.5-inch diskette formatted in an IBM compatible format using Microsoft Word or compatible software. The diskette should be accompanied by a cover letter and should be submitted in "read only" mode. The diskette should be clearly labeled with the commenter's name, proceeding (including the lead docket number, type of pleading (comment or reply comment), date of submission, and the name of the electronic file on the diskette. The label should also include the following phrase "Disk Copy – Not an Original." Each diskette should contain only party's pleading, preferably in a single electronic file. In addition, commenters must send diskette copies to the Commission's copy contractor, Natek Inc., Portals II, 445 12th Street, SW, Room CY-B402, Washington, DC, 20554.

116. Alternative formats (computer diskette, large print, audio cassette and Braille) are available to persons with disabilities by contacting Brian Millin at (202) 418-7426, TTY (202) 418-2555, or via e-mail to Brian.Millin@fcc.gov. This Notice can also be downloaded at http://www.fcc.gov/oet.

V. ORDERING CLAUSES

117. IT IS ORDERED that, pursuant to Sections 4(i), 302, 303(e), 303(f), 303(r) and 307 of the Communications Act of 1934, as amended, 47 U.S.C. Sections 154(i), 302, 303(e), 303(f), 303(r) and 307, this Notice of Proposed Rule Making IS HEREBY ADOPTED.

118. IT IS FURTHER ORDERED that, pursuant to Sections 4(i), 302, 303(e), 303(f), 303(r) and 307 of the Communications Act of 1934, as amended, 47 U.S.C. Sections 154(i), 302, 303(e), 303(f), 303(r) and 307, ET Docket No. 00-47 IS TERMINATED.[127]

119. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this notice, Including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

120. For further information regarding this Notice of Proposed Rule Making, contact Mr. Hugh L. Van Tuyl, (202) 418-7506, e-mail *Hugh.VanTuyl@fcc.gov* or Mr. James Miller, (202) 418-7351, e-mail *James.Miller@fcc.gov*.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[127] *See* paragraph 12 above.

APPENDIX A: PROPOSED RULE CHANGES

Part 2 of Title 47 of the Code of Federal Regulations is proposed to be amended as follows:

1. The authority citation for Part 2 continues to read as follows:

AUTHORITY: 47 U.S.C. 154, 302a, 303 and 336, unless otherwise noted.

2. Section 2.944 is proposed to be revised to read as follows.

§ 2.944 Submission of radio software description.

Applications for certification of software defined radios must include a description and flow diagram of the software that controls the radio frequency operating parameters.

3. Section 2.1033 is proposed to be revised by adding new paragraphs (b)(12) and (c)(18)

§ 2.1033 Application for certification.

* * * * *

(b) * * *

(12) Applications for certification of software defined radios must include the information required by §§ 2.932(e) and 2.944.

(13) Applications for certification of radios operated pursuant to § 90.xxx must demonstrate compliance with the requirements in § 90.yyy.

(c) * * *

(18) Applications for certification of software defined radios must include the information required by §§ 2.932(e) and 2.944.

Part 15 of Title 47 of the Code of Federal Regulations is proposed to be amended as follows:

4. The authority citation of Part 15 continues to read as follows:

AUTHORITY: 47 U.S.C. 154, 302, 303, 304, 307, 336, and 544A.

5. A new Section 15.202 is proposed to be added to read as follows:

§ 15.202 Certified operating frequency range

Certification may be obtained for a device that is capable of operating on frequencies not permitted by this part, provided the device incorporates DFS and operates on only United States frequencies when operated in the United States.

6. A new Section 15.206 is proposed to be added to read as follows:

§ 15.206 Cognitive radio devices

(a) Devices operating under the provisions of § 15.247 may operate with a power level six times greater than the maximum permitted in these sections under the conditions specified in paragraph (c) of this section.

(b) Devices operating under the provisions of 15.249 may operate with a field strength level 2.5 higher than the maximum permitted in this section under the conditions specified in paragraph (c) of this section.

(c) Intentional radiators operating may operate at the higher power limits specified in paragraphs (a) and (b) of this section subject to the following conditions:

(i) Devices must incorporate a mechanism for monitoring the entire band that its transmissions are permitted to occupy.

(ii) Devices must monitor for signals exceeding a monitoring threshold of 30 dB above the thermal noise power within a measurement bandwidth of 1.25 MHz.

(iii) Devices may operate at higher power if signals exceeding the monitoring threshold are detected in less than XX% of the band in which they are permitted to operate

(iv) Devices must incorporate transmit power control to limit their power output to no greater than the maximum normally permitted in §§ 15.247 or 15.249 when the criteria in paragraph (c)(iii) is not met or when higher power operation is not necessary for reliable communications.

7. A new Section 90.xxx is proposed to be added to read as follows:

§ 90.xxx Secondary Leasing of a Public Safety License

Secondary Leasing of a Public Safety License shall operate subject to the following minimum reversion technical requirements:

(1) Devices operating under this rule must employ mechanisms for the immediate, reliable, and secure preemption by and reversion to the primary public safety licensee. Devices must employ such mechanisms as required to ensure they operate lawfully and in compliance with the leasing agreements authorized in this part.

(2) Devices employing a Beacon Signal Detector mechanism as provided in section xx.xxx of this part shall be in compliance with the minimum reversion technical requirements of this rule.

8. A new Section 90.yyy is proposed to be added to read as follows:

§ 90.yyy Technical Requirements: Beacon Signal Detector Leasing Operations

Operations conducted under the rules governing secondary leasing agreements in § xx.xxx of this part may operate subject to a beacon system satisfying the following criteria:

(1) Public Safety licensees shall transmit a beacon signal no less frequently than once per second specifying the frequency or frequencies available for use, the time of day and a secure identifying signature of the Public Safety Licensee Leasor.

(2) Devices operating under § xx.xxx of this part must detect the Public Safety Licensee's beacon signal or cease operations within two seconds. Devices must also incorporate a means to select the transmission frequency specified in the Public Safety Licensee's beacon signal.

APPENDIX B: INITIAL REGULATORY FLEXIBILITY ANALYSIS

As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[128] the Commission has prepared this present Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities small entities by the policies and rules proposed in this Notice of Proposed Rule Making (Notice). Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the Notice provided in paragraph 111 of the item. The Commission will send a copy of the Notice, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[129] In addition, the Notice and IRFA (or summaries thereof) will be published in the Federal Register.[130]

A. Need for, and Objectives of, the Proposed Rules

In the Notice of Proposed Rule Making section, we propose several changes to Parts 2, 15 and other Parts of the rules. Specifically, we propose to:

1) eliminate the requirement for applicants and grantees of equipment authorization to supply a copy of the software that controls the operating parameters of a software defined radio, but add a new requirement that applicants for equipment authorization supply a description and flow diagram showing how the radio software operates
2) require that certain radios that meet the definition of a software defined radio must be declared as such at the time of filing the certification application, and that they must incorporate a means to prevent unauthorized software changes that could change the operating parameters of the radio.
3) permit certification of wireless LAN cards that incorporate additional frequency bands for use in other countries, but limit their operation to authorized frequencies in the United States,
4) permit certain unlicensed devices to operate at higher power levels in areas with limited spectrum use;
5) allow equipment to be developed that could allow public safety entities to lease spectrum on a temporary basis but reclaim it immediately when necessary.

These proposals, if adopted, will prove beneficial to manufacturers and users of unlicensed technology, including those who provide services to rural communities. Specifically, we note that a growing number of wireless internet service providers (WISPs) are using unlicensed devices within wireless networks to serve the needs of consumers. WISPs around the country are providing an alternative high-speed connection in areas where cable or DSL services have been slow to arrive. The higher power limits proposed herein will help to foster a viable last mile solution for delivering Internet services, other data applications, or even video and voice services to underserved, rural, or isolated communities.

[128] *See* 5 U.S.C. § 603. The RFA, *see* 5 U.S.C. § 601 - 612 has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[129] *See* 5 U.S.C. § 603(a).

[130] *See* 5 U.S.C. § 603(a).

These proposals could also benefit public sector entities by allowing the development of "smart" equipment that could enable the leasing of public sector spectrum to generate needed revenue, but would contain safeguards that allow the spectrum to be reclaimed by the public sector entity in the event of an emergency.

B. Legal Basis

The proposed action is authorized under Sections 4(i), 301, 302, 303(e), 303(f), 303(r), 304 and 307 of the Communications Act of 1934, as amended, 47 U.S.C. Sections 154(i), 301, 302, 303(e), 303(f), 303(r), 304 and 307.

C. Description and Estimate of the Number of Small Entities To Which the Proposed Rules Will Apply

The RFA directs agencies to provide a description of, and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules, if adopted.[131] The RFA defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small business concern" under Section 3 of the Small Business Act.[132] Under the Small Business Act, a "small business concern" is one that: (1) is independently owned and operated; (2) is not dominant in its field of operations; and (3) meets may additional criteria established by the Small Business Administration (SBA).[133]

Radio and Television Broadcasting and Wireless Communications Equipment Manufacturers

The Commission has not developed a definition of small entities applicable to unlicensed communications devices manufacturers. Therefore, we will utilize the SBA definition application to manufacturers of Radio and Television Broadcasting and Communications Equipment. Under the SBA's regulations, a Radio and Television Broadcasting and Wireless Communications Equipment Manufacturer must have 750 or fewer employees in order to qualify as a small business concern.[134] Census Bureau data indicates that there are 1,215 U.S. establishments that manufacture radio and television broadcasting and wireless communications equipment, and that 1,150 of these establishments have fewer than 500 employees and would be classified as small entities.[135] The remaining 65 establishments have 500 or more employees; however, we are unable to determine how many of those have fewer than 750 employees and therefore, also qualify as small entities under the SBA definition. We therefore conclude that there are at least 1,150 small manufacturers of radio and television broadcasting

[131] *See* U.S.C. § 603(b)(3).

[132] *Id.* § 601(3).

[133] *Id.* § 632.

[134] 13 C.F.R. § 121.201, NAICS code 334220.

[135] Economics and Statistics Administration, Bureau of Census, U.S. Department of Commerce, 1997 Economic Census, Industry Series - Manufacturing, Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing, Table 4 at 9 (1999). The amount of 500 employees was used to estimate the number of small business firms because the relevant Census categories stopped at 499 employees and began at 500 employees. No category for 750 employees existed. Thus, the number is as accurate as it is possible to calculate with the available information.

and wireless communications equipment, and possibly there are more that operate with more than 500 but fewer than 750 employees.

WISPs and other Wireless Telecommunication Service Providers

The SBA has developed a small business size standard for Cellular and Other Wireless Telecommunication, which consists of all such firms having 1,500 or fewer employees.[136] According to Census Bureau data for 1997, in this category there was a total of 977 firms that operated for the entire year.[137] Of this total, 965 firms had employment of 1,000 employees or more.[138] Thus, under this size standard, the majority of firms can be considered small.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements

Both licensed and unlicensed transmitters are already required to be authorized under the Commission's certification procedure as a prerequisite to marketing and importation, and the proposals in this proceeding would not change that requirement. There would, however, be several changes to the compliance requirements.

Software defined radios in which the software can be easily changed after manufacture would have to be declared as software defined radios at the time the application for certification is filed. This would be a change from the current process, in which declaring a device as a software defined radio is optional. A software defined radio must incorporate security features to prevent unauthorized software changes that affect the operating parameters, and the applicant must describe them in the certification application. We do not expect that this would be a significant compliance burden because manufacturers of radios that would be affected by this requirement generally already take steps to ensure the security of the radio software.

Unlicensed transmitters that would be permitted to operate at higher power in rural and other areas with limited spectrum would have to incorporate sensing capabilities to ensure that higher power operations could occur only in areas where it is permitted. The applicant for certification would have to demonstrate in the application that the equipment meets the requirements.

E. Steps Taken to Minimize Significant Economic Impact on Small Entities, and Significant Alternatives Considered

The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small

[136] 13 C.F.R. § 121.201, NAICS code 517212 (changed from 513322 in October 2002).

[137] U.S. Census Bureau, 1997 Economic Census, Subject Series: Information, "Establishment and Firm Size (Including Legal Form of Organization), "Table 5, NAICS code 513322 (issued October 2000).

[138] *Id.* The census data do not provide a more precise estimate of the number of firms that have 1,500 or fewer employees; the largest category provided is "Firms with 1,000 employees or more."

entities; (3) the use of performance, rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for small entities."[139]

If the rules proposed in this notice are adopted, we believe they would have a significant economic impact on a substantial number of small entities because the rules will impose the following costs: 1) compliance with equipment technical requirements, such as incorporating cognitive capabilities into devices capable of higher power or multi-band operation or using a beacon or other mechanism to enable leased use of spectrum, and 2) compliance with reporting requirements, such as declaring certain radios as software defined radios and supplying certain information about the equipment to the Commission. However, the burdens for complying with the proposed rules would be the same for both large and small entities. Therefore, there would be no differential and adverse impact on smaller entities. Further, the proposals in this *Notice* are beneficial to both large and small entities. Because we believe that the economic impact of the proposed rules on smaller entities would be, in this setting, beneficial rather than adverse, we believe it would be premature to consider specific alternatives to the proposed rules. However, we solicit comment on any such alternatives commenters may wish to suggest for the purpose of facilitating the Commission's intention to minimize any adverse impact on smaller entities.

F. Federal Rules that May Duplicate, Overlap, or Conflict With the Proposed Rule

None.

[139] 5 U.S.C. § 603(c)(1) – (c)(4).

SEPARATE STATEMENT OF CHAIRMAN MICHAEL K. POWELL

Re: Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies (ET Docket No. 03-108); Authorization and Use of Software Defined Radios (ET Docket No. 00-47), Notice of Proposed Rulemaking and Order

Today we take another step forward to improve access and efficiency of our Nation's spectrum and to provide opportunities beyond today's horizon. I am pleased to support this item that grew out of the Spectrum Policy Task Force and that explores the many benefits of smart radio technology and its real-time processing capabilities. Last week, I had the pleasure of visiting several high-tech companies and met with tribal communities that are taking advantage of these new and innovative technologies.

Recent advances in smart radio technologies have the potential to provide more innovative, flexible, and comprehensive use of spectrum while at the same time minimizing the risk of harmful interference. On a real-time basis, smart radios determine their location or environment, have the flexibility to select the best frequencies to use, know how to avoid interference with existing users, and can use vacant spectrum channels. Not only do they have flexibility to use a variety of frequencies, they also can understand and transmit in many different formats.

Smart radio technologies also offer potential solutions to the increasingly crucial interoperability demands facing public safety entities and other licensed users to enable them to coordinate response and recovery efforts and ensure national security. Because they can use different frequencies and modulation techniques, smart radios could also translate signals between two different radio systems. This ability may enable more interoperability between public safety first responders – so that, in an emergency, firefighters from one jurisdiction could more effectively communicate with firefighters in another jurisdiction.

Today's Notice of Proposed Rulemaking and Order is part of a larger effort to expand opportunities for wireless services in rural America. We recently adopted two Notices of Proposed Rulemakings designed to foster advanced telecommunications in rural America. First, an NPRM on how we can clarify rules to minimize regulatory costs and provide incentives to serve rural markets. And second, an NPRM on modified power limits, new technologies such as smart antennas, and streamlined equipment approval.

In this proceeding, we will consider the technical capabilities as well as proposed changes to the Commission's rules and equipment authorization processes to accommodate and enable more efficient use of software defined radio and cognitive radio system technologies. Of special note is the potential of smart radios to facilitate spectrum leasing transactions, including possible leasing of public safety spectrum that would not otherwise be possible without the technology.

The possible uses for smart radios are wide ranging. The challenge before the Commission is to determine how we can open the door for these technologies so as not to shut out any of their tremendous potential.

SEPARATE STATEMENT OF COMMISSIONER MICHAEL J. COPPS

Re: *Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies (ET Docket No. 03-108); Authorization and Use of Software Defined Radios (ET Docket No. 00-47), Notice of Proposed Rule Making and Order*

Cognitive radios have the potential to be a powerful tool for increasing spectral efficiency while keeping interference at acceptably low levels. So, I hope that this NPRM keeps us moving in the direction of allowing consumers and companies to take advantage of these new technologies. I am also eager to explore the idea of allowing higher power levels for unlicensed technologies in rural areas. The wireless networking community has been asking for this for a long time now. If higher powers allow them to bring more service to under-served areas, and more competition to areas largely bereft of competition, we are already late to the game. So I'm glad we're moving forward.

Finally, I want to note that while this NPRM examines technologies that would allow public safety entities such as police departments and fire companies to lease spectrum to non-public-safety users, I will need to be convinced that this is a good idea before voting to allow it. While I want to increase the efficiency of spectrum use in crowded bands, I will need to see proof that allowing commercial operation in the same bands relied on by policemen and firemen is safe. And I will need to be convinced that the lure of big dollar figures from commercial companies will not lead to states and municipalities living in difficult budget environments to lease out not only extra spectrum, but also core spectrum.

SEPARATE STATEMENT OF COMMISSIONER KEVIN J. MARTIN

Re: *Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies (ET Docket No. 03-108); Authorization and Use of Software Defined Radios (ET Docket No. 00-47)*, Notice of Proposed Rulemaking and Order

I am very pleased to support this item, which seeks to facilitate the development of cognitive or "smart" radio technology. Cognitive radio technology has truly great potential to improve spectrum access and efficiency. Among other things, the technology allows for greater sharing of spectrum. As I have previously discussed, promoting spectrum sharing is a fundamental part of encouraging efficient spectrum usage. *See, e.g.*, Remarks by Kevin J. Martin to the FCBA Policy Summit & CLE, *U.S. Spectrum Policy: Convergence or Co-Existence?* (Mar. 5, 2002). While the amount of available spectrum is ultimately limited only by technology, the spectrum supply currently feels very limited. Sharing spectrum is a crucial means to get more mileage out of this important resource. *See id.* Cognitive radio technology allows for greater spectrum sharing by enabling devices to find and use available spectrum in different frequencies, times, or spaces. This can be as simple as frequency hopping in a wireless local area network or as advanced as DARPA's XG program, which would allow multiple users to share common spectrum by avoiding conflicts in time, frequency, code, and other signal characteristics. I am confident that we will see even greater advances in spectrum sharing through cognitive radio technology, and the Commission should do what it can to facilitate such advances.

Cognitive radio technology also makes possible improved spectrum access in rural areas. Many Wireless Internet Service Providers (WISPs) are using unlicensed spectrum to provide innovative services in rural areas but are finding it difficult to provide adequate signal coverage because of our current Part 15 power limits. This item proposes allowing such providers to increase their power input if they use cognitive radio technology to avoid interference to other users. I am very supportive of this proposal, and I look forward to receiving comments.

Cognitive radio technology also has great potential for enabling interoperability among public safety agencies. Lack of interoperability has been identified as a significant problem in our response to the September 11 attacks and in other disasters involving multiple jurisdictions, and we must all focus on improving interoperability. Cognitive radio technology can play an important part in that improvement by enabling devices to bridge communications between jurisdictions using different frequencies and modulation formats. Through such a mechanism, a fire department from Long Island could communicate effectively with a police department from Manhattan even if they use completely different radio systems. Such interoperability is crucial to enabling public safety agencies to do their jobs.

Accordingly, for all of these reasons, I look forward to receiving comment on how we can best promote cognitive radio technology.